

500.42806X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): A. OKUYAMAI, et al
Serial No.:
Filed: June 24, 2003
Title: INFORMATION RECORDING/REPRODUCING SYSTEM
Group:

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

June 24, 2003

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 2002-182325 filed June 24, 2002.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Melvin Kraus
Registration No. 22,466

MK/nac
Attachment
(703) 312-6600

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 6月24日

出 願 番 号

Application Number:

特願2002-182325

[ST.10/C]:

[JP2002-182325]

出 願 人

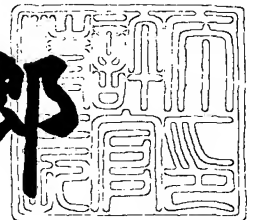
Applicant(s):

株式会社日立製作所

2003年 4月 8日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3024352

【書類名】 特許願

【整理番号】 1502001481

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 13/36

【発明者】

【住所又は居所】 茨城県土浦市神立町 5 0 2 番地 株式会社 日立製作所
機械研究所内

【氏名】 奥山 淳

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社
日立製作所 システム開発研究所内

【氏名】 道明 誠一

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社
日立製作所 システム開発研究所内

【氏名】 小川 仁

【発明者】

【住所又は居所】 茨城県土浦市神立町 5 0 2 番地 株式会社 日立製作所
機械研究所内

【氏名】 薄井 和明

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【電話番号】 03-3212-1111

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録再生システム

【特許請求の範囲】

【請求項 1】

情報を記録再生する磁気ディスク装置と、該磁気ディスク装置を着脱可能に接続し該磁気ディスク装置に対して情報の記録再生のためのアクセスを行なうホストシステムとを有する情報記録再生システムにおいて、

前記磁気ディスク装置は、自身の物理的な特性に基づき認証鍵を作成する認証鍵作成手段を有することを特徴とする情報記録再生システム。

【請求項 2】

前記磁気ディスク装置及び前記ホストシステムは、前記認証鍵を記録する認証鍵記録手段をそれぞれ有すると共に、前記認証鍵に基づき認証データを作成する認証データ作成手段をそれぞれ有し、前記ホストシステムの認証データと、前記磁気ディスク装置の認証データとに基づいて、前記ホストシステムからの前記磁気ディスク装置の情報へのアクセスを制御するアクセス制御手段を少なくとも一つ有することを特徴とする請求項 1 に記載の情報記録再生システム。

【請求項 3】

前記認証鍵は、前記磁気ディスク装置が有する磁気ディスクの媒体欠陥特性に基づき作成することを特徴とする請求項 1 に記載の情報記録再生システム。

【請求項 4】

前記認証鍵は、前記磁気ディスク装置が有する磁気ディスクの偏心特性に基づき作成することを特徴とする請求項 1 に記載の情報記録再生システム。

【請求項 5】

前記認証鍵は、前記磁気ディスク装置が有する磁気ディスクの偏心特性を補償する偏心補償信号に基づき作成することを特徴とする請求項 1 に記載の情報記録再生システム。

【請求項 6】

前記認証鍵は、前記磁気ディスク装置が有する磁気ディスクの偏心特性を補償する偏心補償信号をウェーブレット変換した結果に基づき作成することを特徴とす

る請求項 1 に記載の情報記録再生システム。

【請求項 7】

前記認証鍵は、3 個所以内のそれぞれ異なるシリンダで作成された偏心補償信号に基づき作成することを特徴とする請求項 1 に記載の情報記録再生システム。

【請求項 8】

前記磁気ディスク装置は、前記磁気ディスク装置が有する磁気ディスクの偏心を補償する偏心補償信号を作成する手段と、前記認証鍵に基づき前記偏心補償信号を暗号化する手段と、暗号化された前記偏心補償信号を記録する手段と、暗号化された前記偏心補償信号を前記認証鍵に基づき暗号化前の偏心補償信号に戻す手段とを有することを特徴とする請求項 1 に記載の情報記録再生システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報を記録再生する磁気ディスク装置とこの磁気ディスク装置を着脱可能に接続してアクセスを行なうホストシステムとを有する情報記録再生システムに関し、磁気ディスク装置にアクセスするホストシステムを特定のものに限定可能とする情報記録再生システムに関する。

【0002】

【従来の技術】

磁気ディスク装置をホストシステムから着脱可能にして、音楽サーバ、ビデオレコーダ、携帯情報端末、カーナビゲーションなどで動画や音声といったデータを記録再生する用途として使用するシステムが提案されている。着脱可能な構成であるため、第三者が不当に磁気ディスク装置を取り外し、別のホストシステムで情報を読み書きする等のセキュリティ上の問題が考えられる。磁気ディスク装置とホストシステムの組み合わせを限定する技術としては、認証データを用いた相互認証処理がある。例えば、特開 2 0 0 1 - 2 5 6 0 0 4 号公報では、記憶装置或いはホストシステム的一方で作成された認証データに基づいて他方がアクセス制御用の認証データを作成し、この認証データを用いてホストシステムのアクセス制御を行なう技術を開示している。認証データは、記憶装置或いはホストシ

システムの固有情報と日時情報に基づいて作成される。固有情報としては、メーカー名、機種名、シリアル番号を使用している。

【 0 0 0 3 】

【発明が解決しようとする課題】

特開 2 0 0 1 - 2 5 6 0 0 4 号公報の技術では、容易に入手できる情報を用いているため、認証鍵を予測できる可能性がある。また、不正なユーザによって、ある 1 つの装置から認証鍵を取得されてしまった場合、メーカー名、機種名、シリアル番号に基づき別の装置の認証鍵も容易に予測できる可能性がある。

【 0 0 0 4 】

本発明の目的は、予測が困難な認証鍵によって相互認証を行うことにより、磁気ディスク装置とホストシステムとを特定の組み合わせに限定することが可能なシステムを提供することにある。

【 0 0 0 5 】

【課題を解決するための手段】

本発明の情報記録再生システムは、磁気ディスク装置及びホストシステムの各々の認証鍵記憶手段に、磁気ディスク装置の物理的な特性に基づき作成する認証鍵を記録する。認証鍵は、例えば磁気ディスク装置が有する磁気ディスクの媒体欠陥特性或いは偏心特性に基づいて作成するとよい。更に、磁気ディスク装置及びホストシステムは、前記認証鍵を使用して認証データを作成する。そして、磁気ディスク装置のアクセス制御手段において、ホストシステムで作成された認証データと、磁気ディスク装置で作成された認証データとに基づいて、磁気ディスク装置へのアクセスを特定のホストシステムのみに限定するよう制御する。或いは、ホストシステムのアクセス制御手段において、磁気ディスク装置で作成された認証データと、ホストシステムで作成された認証データとに基づいて、ホストシステムを特定の磁気ディスク装置のみに限定してアクセスを行うように制御する。

磁気ディスクの媒体欠陥特性或いは偏心特性の発生は、人間の手が介在していない。また、それぞれの磁気ディスク装置毎に特性が異なる。従って、磁気ディスクの媒体欠陥特性或いは偏心特性から作成される認証鍵は、人間の指紋のよう

にそれぞれの磁気ディスク装置毎に異なり、予測は極めて困難である。

【 0 0 0 6 】

【発明の実施の形態】

以下、本発明の実施形態について図面を用いて説明する。

【 0 0 0 7 】

図 1 は、本発明の実施形態による情報記録再生システムの構成図の一例である。本情報記録再生システムは、磁気ディスク装置 1 0 0 とホストシステム 1 0 1 とからなる。磁気ディスク 1 は、スピンドルモータ（S P M）2 により回転される。なお、磁気ディスク 1 の各トラック（図示せず）には、サーボ情報が記録されたサーボ領域と、データを記録するためのデータ領域とを有する。磁気ヘッド 3 は、アクチュエータ 4 に搭載されて、磁気ディスク 1 の半径方向に移動される。アクチュエータ 4 はボイスコイルモータ（V C M）5 を駆動源として構成されている。S P M 2 及び V C M 5 は、後述する C P U 9 の制御により、V C M / S P M ドライバ 6 から駆動電流を供給されて駆動する。V C M / S P M ドライバ 6 は、通常では C P U 9 からゲートアレイ 7 を介してデジタル制御値を入力し、当該制御値に応じて駆動電流を出力する。リード／ライト回路（R / W 回路）8 は、磁気ヘッド 3 の信号からリード信号を復調したり、磁気ヘッド 3 にライト信号を供給する。なお、R / W 回路 8 は、サーボ情報から磁気ヘッド 3 の位置を検出する位置検出回路（図示せず）を有する。H D C 1 2 は、ホストシステム 1 0 1 との間でのデータ転送を制御するものであり、ホストシステム 1 0 1 から入力されるデータを一時的にランダムアクセスメモリ（R A M）1 1 に記憶させる等といった制御を行なう。セントラルコントロールユニット（C P U）9 は、リードオンリーメモリ（R O M）1 0 に格納された制御プログラムに従って、アクチュエータの制御等を行なう。1 3 は認証鍵作成手段、1 4 は認証鍵記録手段、1 5 は認証データ作成手段、1 6 はアクセス制御手段である。これらの詳細については後述する。ゲートアレイ 7、R / W 回路 8、C P U 9、R O M 1 0、R A M 1 1、H D C 1 2、認証鍵作成手段 1 3、認証鍵記録手段 1 4、認証データ作成手段 1 5、アクセス制御手段 1 6 は、それぞれバスで接続されている。本実施形態の磁気ディスク装置 1 0 0 は、従来の磁気ディスク装置と言われている情報を

磁気ディスクに記録再生する情報記録再生部に加えて、認証鍵作成手段 1 3、認証鍵記録手段 1 4、認証データ作成手段 1 5、アクセス制御手段 1 6 とを備えたものである。

【 0 0 0 8 】

1 7 はインターフェース (I / F) 回路、1 8 は CPU、1 9 は ROM、2 0 は RAM、2 1 は認証鍵記録手段、2 2 は認証データ作成手段、2 3 はアクセス制御手段である。なお、ホストシステム 1 0 1 は、パーソナルコンピュータ、音楽サーバ、ビデオレコーダ、携帯情報端末、カーナビゲーションなどを想定しており、必ずしも上記の各要素の全てを含まなくとも良い。

次に、認証鍵作成手段 1 3 の一例について説明する。通常、磁気ディスク装置の記録再生処理は、記録媒体である磁気ディスクのデータ記録領域に設定されたセクタを最小単位として行われる。このとき、磁気ディスクのデータ記録領域に設定された多数のセクタの中には、磁気ディスクに付着した塵埃や組み立て工程時の損傷等の影響を受けて、データの書き込みや読み出しが正常に行なわれないセクタが存在する場合がある。このようなセクタは欠陥セクタと呼ばれている。磁気ディスクに記録するデータの信頼性を確保する上では、上記のような欠陥セクタを適切に検出して、この欠陥セクタにはデータの記録を行なわないことが望まれる。そこで、磁気ディスクに対してデータの記録再生を行なう際は、一般に、ディフェクト管理と呼ばれる欠陥セクタを管理するための処理が行われている。

【 0 0 0 9 】

磁気ディスク上に発生する欠陥は、磁気ディスク初期化の際に発見される 1 次欠陥と、磁気ディスクへのデータ記録終了後に記録したデータを再度読み取りして正しい記録が行われたかを判定するいわゆるベリファイを行なった際に発見される 2 次欠陥とに分けられる。ディフェクト管理を行なう場合、磁気ディスクのデータ記録領域には、欠陥セクタについての情報をテーブル化して書き込んでおくためのディフェクト管理エリア (DMA) と呼ばれる領域が設けられる。そして、欠陥セクタが検出された場合には、この欠陥セクタの位置情報等がこの DMA に書き込まれる。一般に、1 次欠陥は DMA の PDL (P r i m a r y D e

fect List) と呼ばれる部分に書き込まれ、2次欠陥はDMAのSDL (Secondary Defect List) と呼ばれる部分に書き込まれる。

【0010】

図2に、欠陥セクタ情報の位置を表す欠陥配置図の一例を示す。縦軸は磁気ヘッドのヘッド番号、横軸は磁気ディスク装置のセクタ番号である。図2では、磁気ヘッドのヘッド番号を0～3とし、セクタ番号を0～5としている。なお、今後、図2のテーブルの各要素の場所は、(ヘッド番号、セクタ番号)のようにヘッド番号とセクタ番号の指定で表すことにする。欠陥セクタが検出されない場合は、(0, 0)から(0, 5)までのテーブルに、論理値0～5を格納する。次に、(1, 0)から次の論理値6を格納して行く。欠陥セクタが検出された場合は、欠陥の種類を区別できる情報を格納する。欠陥の種類としては、欠陥部分を飛ばして追従するスリップディフェクトと、欠陥を他のテーブルに移動させる交代ディフェクトが存在する。スリップディフェクトは、図2の(1, 1)と(2, 5)に示すように、先頭にSを付加する。交代ディフェクトは、図2の(2, 3)に示すように、先頭にRを付加する。また、欠陥の番号は、論理値の順に1から付加する。

【0011】

図3に、欠陥管理テーブルの一例を示す。図3は、図2の欠陥配置図から各欠陥のヘッド番号とセクタ番号を抜き出して表示したものである。スリップディフェクトであるS1とS3は、その情報が格納されているヘッド番号とセクタ番号を示している。交代ディフェクトであるR2は、元の位置のヘッド番号とセクタ番号、移動先のヘッド番号とセクタ番号を示している。

【0012】

認証鍵を、上記欠陥管理テーブルを基に作成する。図4に、認証鍵作成の手順を示すフローチャートの一例を示す。ホストシステム101から認証鍵作成の要求コマンドを受け取った場合(200)、欠陥管理テーブルを基に認証鍵を作成する(201)。欠陥管理テーブルから値を選択し、2進数に変換し、例えば256ビット以内の56ビットや128ビットの認証鍵を作成する。欠陥管理テ

ブル値の選択は、どのような規則に従って選んでもかまわない。また、欠陥管理テーブル値を、DMAのPDLだけから読み出すことにして、1次欠陥の値だけから選ぶことも可能である。更にまた、後述する認証データ作成手段15、22で認証データを作成する際に必要とする認証鍵の数に合わせて、複数の認証鍵を作成することも可能である。

【0013】

作成した認証鍵は、ホストシステム101に送信するとともに(202)、認証鍵記録手段14に記録する(203)。また、ホストシステム101は、受信した認証鍵を認証鍵記録手段21に記録する。欠陥の特徴として、磁気ディスク装置毎に欠陥の種類や場所が異なっているということが上げられる。また、欠陥の発生に人間の手が介在していないということが上げられる。従って、複製は不可能であり、不正な改ざん等に対して強固な認証鍵として使用できる。更に、今後、磁気ディスク装置の記録密度が向上し、データ記録密度が向上するほど欠陥の数は増加すると考えられる。従って、磁気ディスク装置の記録密度向上に対応して、不正な改ざん等に対してより強固な認証鍵を作成することが可能となる。

【0014】

次に、認証鍵作成手段13の別の一例について説明する。通常、磁気ヘッドを追従させるべき磁気ディスク上のトラックには、特にディスクの回転に伴う要因により偏心が発生する。要因としては、磁気ディスクを回転させるためのSPMの軸振れ、サーボ情報を書き込む時の磁気ディスクの振動等がある。また、磁気ディスク上にサーボ情報を書き込む時に、磁気ディスクを実装する磁気ディスク装置自体ではなく、サーボライターと呼ばれる専用のサーボ情報書き込み装置を使用することがある。このような場合には、サーボ情報を書き込みした磁気ディスクを磁気ディスク装置に装着した時に、SPMの回転中心と、サーボライターによりサーボ情報を書き込みした時の磁気ディスクの取り付け位置での回転中心との誤差により、巨大な偏心が発生する可能性がある。このようなトラック偏心に伴う振幅は、磁気ヘッドの位置誤差量に換算して、数十 μ m程度になることもある。なお、ディスク偏心特性は、1台の磁気ディスク装置でもトラック毎に特性が異なる。

【 0 0 1 5 】

高トラック密度化を図る磁気ディスク装置では、確実にデータを記録再生するための誤差の許容範囲は0。数 μ m程度である。誤差がこの許容範囲を越える場合には、磁気ヘッドを目標トラックに追従させることが困難となる。そのため、一般的に、ディスク偏心特性を検出して偏心による位置誤差を低減する偏心補償信号を作成し、ヘッド位置決め制御系において偏心の影響を補償している。偏心補償信号を作成する方法は、繰り返し制御に基づく方法、フーリエ級数展開に基づく方法、外乱オブザーバに基づく方法等、多くの方法が提案されている。偏心補償は、リアルタイムに偏心補償を行う方式と、偏心補償信号に基づき予めテーブルを作成しておき、サーボセクタ番号に基づきテーブル値を読み出すテーブル参照方式とに大別できる。ただし、磁気ディスクの回転周波数の数倍程度の低次の偏心特性は、周囲環境温度などの使用条件の影響を受けて、変動する場合が考えられる。そこで、一般的には、低次の偏心はリアルタイムに偏心補償信号を作成して補償される。

【 0 0 1 6 】

認証鍵を、上記偏心補償信号を基に作成する。図5に、ヘッド位置決め制御系のブロック線図の一例を示す。また、図6に、認証鍵作成の手順を示すフローチャートの一例を示す。ヘッド位置決め制御系は、磁気ヘッド3が読み出したサーボ情報から検出される磁気ヘッド3の位置信号に基づき、フィードバック制御系が構成されている。それぞれ具体的には、制御対象は図1のVCM5等から構成される磁気ヘッド3の移動機構であり、コントローラ、第1の偏心補償手段、第2の偏心補償手段、平均化手段はCPU9で演算されるプログラム或いはハードロジックである。また、記憶手段は、ROM10やRAM11等のメモリであればよく、或いは磁気ディスク1の特定の記録領域とすることも可能である。特定の記憶領域とは、通常のデータの記録動作では書き換え不可能（アクセス不可能）な例えば代替セクタ（冗長記録領域）やサーボ領域を想定する。

【 0 0 1 7 】

変動する場合が考えられる低次の偏心特性はリアルタイムに第1の偏心補償手段で補償し、それ以外の偏心特性は第2の偏心補償手段によりテーブル参照方式

で補償する。ただし、第2の偏心補償信号は、例えばディスク4回転分の第2の偏心補償信号の同一サーボセクタ番号の値に対して平均化処理を行い、記憶手段に記憶する。このとき、ノイズ対策等の目的でフィルタ処理を併用してもよい。平均化された第2の偏心補償信号は、サーボセクタ番号に基づき読み出される。偏心補償手段は、偏心補償信号を作成することができるのならば、どのような方法でもかまわない。また、操作信号に基づき偏心補償信号を作成し、作成した偏心補償信号を操作信号に加算する方式でも同様な手順で行うことができる。

【0018】

ホストシステム101から認証鍵作成の要求コマンドを受け取った場合(300)、目標シリンダとヘッド番号を設定し(301)、シークを行う(302)。次に、目標シリンダにシーク後、第1の偏心補償信号の過渡特性が収束するまで例えばディスク4回転分待ち、その後、平均化された第2の偏心補償信号を作成する(303)。次に、平均化された第2の偏心補償信号を基にして、周囲環境温度などの使用条件の影響を受けない高次成分を取り出すための処理を行う。例えば、ハイパスフィルタ処理を行い第2の偏心補償信号から高次成分を取り出す。なお、フィルタ特性は、位相が0或いは群遅延特性が一定であることが望ましい。また、ウェーブレット変換を行い第2の偏心補償信号から高次成分を取り出す。例えば、多重解像度解析を行ない、第1回目のウェーブレット分解のハイパス要素を用いてもよい。更に、第2回目以降のウェーブレット分解結果を用いてもよい。また、ウェーブレットパケット解析を行ない、第1回目のウェーブレットパケット分解のハイパス要素を用いてもよい。更に、第2回目以降のウェーブレットパケット分解結果を用いてもよい。

【0019】

301から304までの処理は、適当な回数だけ行う(305)。例えば、1トラックにサーボセクタ数が100個の場合、301から304までの処理を目標シリンダを変えながら3回行うことにより、300個の平均化された第2の偏心補償信号値が作成される。この300個の平均化された第2の偏心補償信号値から値を選択し、2進数に変換し、例えば256ビット以内の56ビットや128ビットの認証鍵を作成する(306)。目標シリンダの選択は、どのような規

則に従って選んでもかまわない。また、2進数に変換する値の選択は、どのような規則に従って選んでもかまわない。更にまた、後述する認証データ作成手段15、22で認証データを作成する際に必要とする認証鍵の数に合わせて、複数の認証鍵を作成することも可能である。

【0020】

作成した認証鍵は、ホストシステム101に送信するとともに(307)、認証鍵記録手段14に記録する(308)。また、ホストシステム101は、受信した認証鍵を認証鍵記録手段21に記録する。

【0021】

偏心の特徴として、磁気ディスク装置毎に特性が異なっているということが上げられる。また、偏心の発生に人間の手が介在していないということが上げられる。従って、複製は不可能であり、不正な改ざん等に対して強固な認証鍵として使用できる。更に、今後、磁気ディスク装置の記録密度が向上し、トラック密度が向上するほどサーボセクタ数は増加すると考えられる。従って、磁気ディスク装置の記録密度向上に対応して、不正な改ざん等に対してより強固な認証鍵を作成することが可能となる。

【0022】

これらの認証鍵は、認証鍵記録手段14と21に記録される。認証鍵記録手段14と21は、ROM等のメモリであれば良い。なお、認証鍵記録手段14をROM10で代用し、認証鍵記録手段21をROM19で代用することも可能である。更に、磁気ディスク1の特定の記録領域に記録することも可能である。特定の記憶領域とは、通常データの記録動作では書き換え不可能(アクセス不可能)な例えば代替セクタ(冗長記録領域)やサーボ領域を想定する。これらを併用することにより、改ざん等に対してより強固な認証鍵とすることも可能である。

【0023】

図4或いは6の手順で認証鍵を作成する時期としては、組み合わせを限定する目的で磁気ディスク装置がホストシステムに装着されたときに認証鍵を作成してもよい。例えば、磁気ディスク装置側に初めて認証鍵を作成すると1になるフラグを用意する。すなわち、1度でも認証鍵を作成したことがある場合は、それ以

後上記フラグは1のままになる。このフラグは、通常のデータの記録動作では書き換え不可能（アクセス不可能）な例えば代替セクタ（冗長記録領域）やサーボ領域に作成されることが望ましい。

【0024】

ホストシステムは、磁気ディスク装置が装着されたときに、磁気ディスク装置に上記フラグ情報を確認してその結果を送信するように要求し、上記フラグが0の場合は磁気ディスク装置に認証鍵を作成して送信することを要求するコマンドを送信する。また、組み合わせを限定する目的で磁気ディスク装置がホストシステムに装着されたとき、例えばユーザにより、ホストシステムに認証鍵の作成を要求するコマンドを入力させてもよい。

【0025】

ホストシステムは、認証鍵の作成を要求するコマンドが入力された場合、磁気ディスク装置に認証鍵を作成して送信することを要求するコマンドを送信する。この際、例えば、ホストシステム側でユーザからの認証鍵作成要求の回数を管理して、ユーザが認証鍵の作成を要求できる回数に制限を持たせておくことが望ましい。更にまた、磁気ディスク装置とホストシステムとを有する情報記録再生システムを停止する際、認証鍵を作成してもよい。

【0026】

ホストシステムが停止命令を受けた場合、磁気ディスク装置に認証鍵を作成して送信することを要求するコマンドを送信する。この際、例えば、ホストシステム側から認証鍵の受信完了を示すフラグを磁気ディスク装置に送信し、磁気ディスク装置はそのフラグを受信してから停止し、ホストシステムはフラグ送信後から磁気ディスク装置が停止完了する一定時間経過後に停止することが望ましい。この場合、次回起動時における認証鍵は、前回稼動中に欠陥特性或いは偏心特性が何らかの理由により変化したとしても、その変化を反映した値に更新されている。また、起動毎に異なる認証鍵を用いることになり、不正な改ざん等に対してより強固となる。

【0027】

次に、磁気ディスク装置100とホストシステム101の認証手順について説

明する。図7は、ホストシステム101側から磁気ディスク装置100の認証を行なう手順を示すフローチャートの一例である。図8は、ホストシステム101から認証開始のコマンドを受信した場合の磁気ディスク装置100側の手順を示すフローチャートの一例である。

【0028】

まず、ホストシステム101側の手順について説明する。ホストシステム101は、認証開始を示すコマンドを磁気ディスク装置100に送信する(401)。次に、認証データの元になるデータを作成し(402)、磁気ディスク装置100に送信する(403)。このデータは、適当なランダムデータであればよい。次に、このデータを、ホストシステム101が有する認証鍵を使って暗号化し(404)、磁気ディスク装置100から暗号文が送られてくるまで待機する(405)。磁気ディスク装置100から暗号文を受信したら、ホストシステム101の暗号文と磁気ディスク装置100の暗号文を比較し(406)、一致すれば磁気ディスク装置100の認証成立とし(407)、一致しなければ磁気ディスク装置100の認証不成立とする(408)。

【0029】

次に、磁気ディスク装置100側の手順について説明する。認証開始のコマンド入力を受信した場合(500)、ホストシステム101から送られてくるデータを受信する(501)。次に、502から507までの手順により、認証鍵を作成する。この手順は、図6の301から306までの手順と同様であるので説明は省略する。なお、502から507までの手順に変わり、欠陥特性に基づく認証鍵を使用する場合などは、認証鍵記録手段14に記録された認証鍵を読み出す手順としてもよい。

【0030】

次に、認証鍵を使ってデータを暗号化し(508)、ホストシステム101に暗号文を送信する(509)。これにより、406で暗号文が一致すれば、ホストシステム101と磁気ディスク装置100は同一の暗号鍵を有していることになるので認証が成立する。また、磁気ディスク装置100をホストシステム101と読み替えて図7の処理を磁気ディスク装置100側で行ない、ホストシステ

ム 1 0 1 を磁気ディスク装置 1 0 0 と読み替えて図 8 の処理をホストシステム 1 0 1 側で行なえば、磁気ディスク装置 1 0 0 側からホストシステム 1 0 1 を認証することができる。この場合、5 0 2 から 5 0 7 までの手順は、認証鍵記録手段 2 1 に記録された認証鍵を読み出す手順となる。なお、上記で、認証鍵を使ってデータを暗号化する処理は、認証データ作成手段 1 5 と 2 2 で行なっている。

【 0 0 3 1 】

また、暗号文の比較を行なうことにより認証の成立、不成立を判断する処理は、アクセス制御手段 1 6 と 2 3 で行なっている。認証データ作成手段 1 5 と 2 2 は、認証鍵を利用してデータを暗号化できるものであればどのようなものでもかまわない。また、アクセス制御手段 1 6 と 2 3 は、暗号文の比較を行ない、同一かどうかを判断できるものであればどのようなものでもかまわない。例えば、暗号文を 2 進数に変換して論理積を計算し、結果が 1 であれば暗号文は一致している。

【 0 0 3 2 】

磁気ディスク装置 1 0 0 側でホストシステム 1 0 0 の認証が成立した場合はホストシステム 1 0 1 からのアクセスを許可し、認証が不成立の場合はホストシステム 1 0 1 からのアクセスを不許可にする。また、ホストシステム 1 0 1 側で磁気ディスク装置 1 0 0 の認証が成立した場合は磁気ディスク装置 1 0 0 にアクセスを行なえるようにし、認証が不成立の場合は磁気ディスク装置 1 0 0 にアクセスを行なわないようにする。また、ホストシステム 1 0 1 側で磁気ディスク装置 1 0 0 の認証が不成立の場合は、その旨をユーザに通知してもよい。この相互認証により、ホストシステム 1 0 1 と磁気ディスク装置 1 0 0 の組み合わせを限定することができる。

【 0 0 3 3 】

次に、ホストシステム 1 0 1 と磁気ディスク装置 1 0 0 の組み合わせを限定する別の一例について説明する。図 9 に、ヘッド位置決め制御系のブロック線図の一例を示す。また、図 1 0 に、第 2 の偏心補償信号の作成手順を示すフローチャートの一例を示す。

【 0 0 3 4 】

図9は、図5のヘッド位置決め制御系のブロック線図に対して、暗号化手段と復号化手段を加えたものである。まず、ホストシステム101から第2の偏心補償信号の作成を要求するコマンドを受信した場合(600)、目標シリンダを設定し(601から603)、シークを行なう(604)。次に、目標シリンダで平均化された第2の偏心補償信号を作成する(605)。次に、作成した第2の偏心補償信号を認証鍵を使って暗号化し(606)、記憶する(607)。ここまでの処理を、全てのシリンダで行う(608)。記憶した第2の偏心補償信号を使用する場合は、復号化手段で認証鍵を利用して暗号化前の第2の偏心補償信号に戻して使用する。ただし、復号化手段で使用する認証鍵は、ホストシステム101から受信した認証鍵を用いる。従って、磁気ディスク装置100は、ホストシステム101から正しい認証鍵を受信しない限り、第2の偏心補償信号を利用することができない。そこで、例えば、磁気ディスク装置とホストシステムとを有する情報記録再生システムの起動時に、ホストシステムから磁気ディスク装置に認証鍵を送信するようにする。こうすることにより、同一の認証鍵を有するホストシステムと磁気ディスク装置の組み合わせでない限り、磁気ディスク装置は正しい第2の偏心補償信号を利用できないのでヘッド追従誤差が増加し、正常な記録再生動作を行なうことができない。従って、ホストシステム101と磁気ディスク装置100の組み合わせを限定することができる。

【0035】

なお、上記本実施形態では、磁気ディスク装置100のインターフェースとして、ATA(AT ATTACHMENT)規格を想定している。しかし、例えば、SCSI(Small Computer System Interface)等にも適用可能である。ホストシステム101から例えば認証鍵の取得は、ATA規格を利用して行っても良いし、その他の方法で行っても良い。ATA規格を利用する一例としては、Set Featuresコマンド(或いはIdentify Deviceコマンド)を利用して認証鍵の取得を行う。ATA規格で規定されている同コマンドに対して、例えばベンダユニーク領域或いはリザーブ領域に認証鍵の送信開始を示すビットを設ける。ホストシステム101(或いは磁気ディスク装置100)はSet Featuresコマンド(或いは

Identify Device コマンド) の発行と認証鍵の送信を示すビットを監視していて、例えばビットが 1 の場合は、磁気ディスク装置 1 0 0 (或いはホストシステム 1 0 1) に認証鍵を送信する。

【 0 0 3 6 】

以上説明したように、磁気ディスク装置 1 0 0 とホストシステム 1 0 1 との間で、磁気ディスク装置の物理的な特性に基づき作成する認証データを用いて互いの認証を行うようにしたため、磁気ディスク装置側においては、当該磁気ディスク装置へのアクセスを特定のホストシステムのみに限定するように制御でき、また、ホストシステム側においては、特定の磁気ディスク装置のみに限定してアクセスを行うように制御することが可能となる。

【 0 0 3 7 】

【発明の効果】

以上、本発明では、磁気ディスク装置の物理的な特性に基づいて認証データを作成することにより、認証データの予測が極めて困難であり、このような認証データを用いて相互認証を行うことにより、磁気ディスク装置とホストシステムとを特定の組み合わせに限定することが可能である。

【図面の簡単な説明】

【図 1】 本発明の実施形態による情報記録再生システムの構成図である。

【図 2】 欠陥配置図の一例である。

【図 3】 欠陥管理テーブルの一例である。

【図 4】 認証鍵の作成手順を示すフローチャートの一例である。

【図 5】 ヘッド位置決め制御系のブロック線図の一例である。

【図 6】 認証鍵の作成手順を示すフローチャートの一例である。

【図 7】 認証処理の手順を示すフローチャートの一例である。

【図 8】 認証処理の手順を示すフローチャートの一例である。

【図 9】 ヘッド位置決め制御系のブロック線図の一例である。

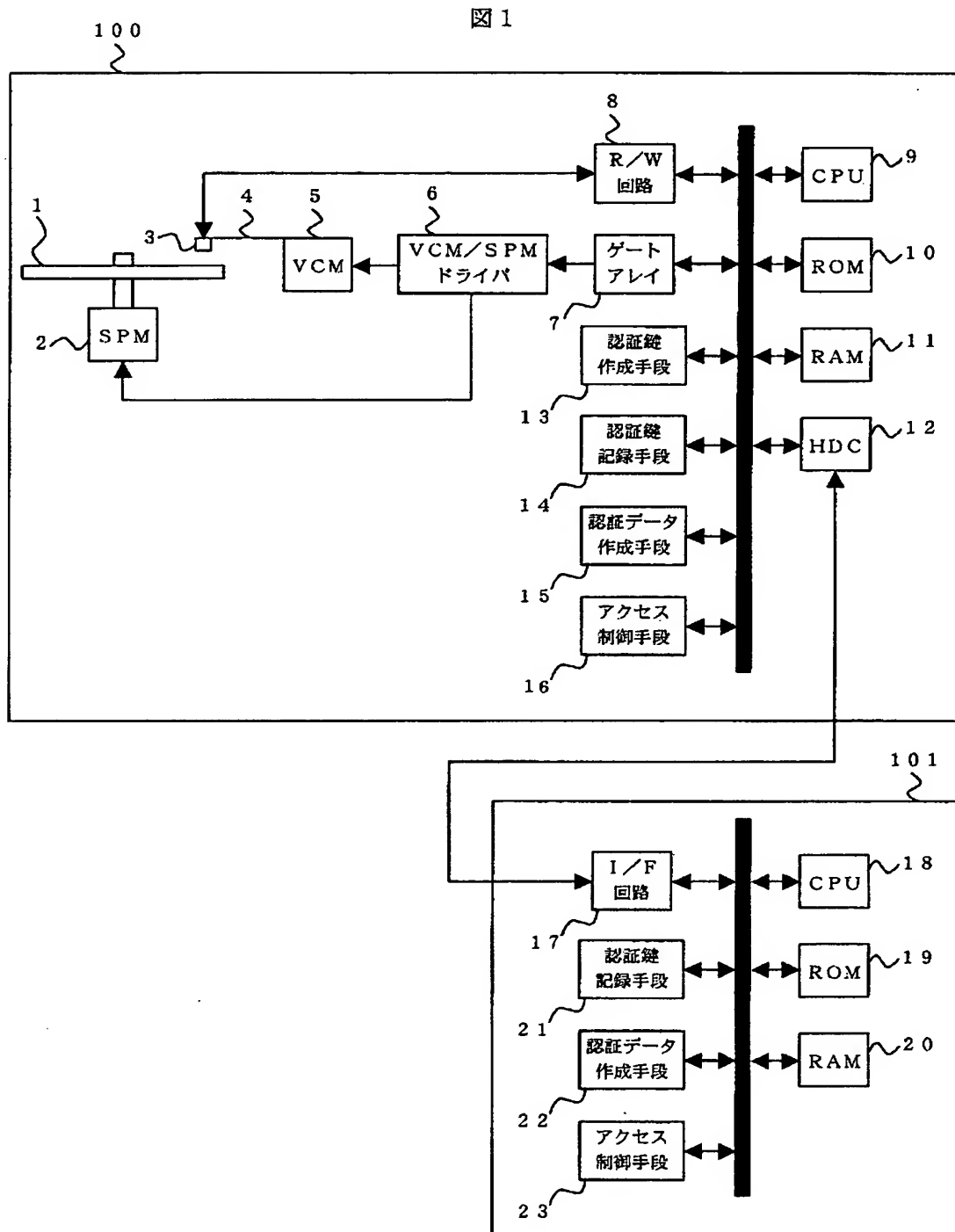
【図 1 0】 第 2 の偏心補償信号の作成手順を示すフローチャートの一例である。

【符号の説明】

1…磁気ディスク、2…SPM、3…磁気ヘッド、4…アクチュエータ、5…VCM、6…VCM／SPMドライバ、7…ゲートアレイ、8…R／W回路、9…CPU、10…ROM、11…RAM、12…HDC、13…認証鍵作成手段、14…認証鍵記録手段、15…認証データ作成手段、16…アクセス制御手段、17…I／F回路、18…CPU、19…ROM、20…RAM、21…認証鍵記録手段、22…認証データ作成手段、23…アクセス制御手段。

【書類名】 図面

【図 1】



【図 2】

図 2

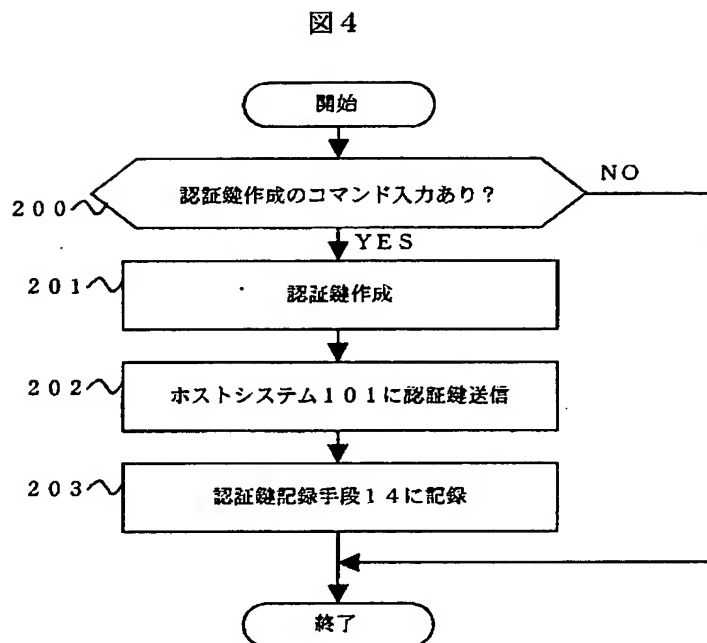
セクタ番号 ヘッド番号	0	1	2	3	4	5
0	0	1	2	3	4	5
1	6	S 1	7	8	9	1 0
2	1 1	1 2	1 3	R 2	1 5	S 3
3	1 6	1 7	1 8	1 9	1 4	S P

【図 3】

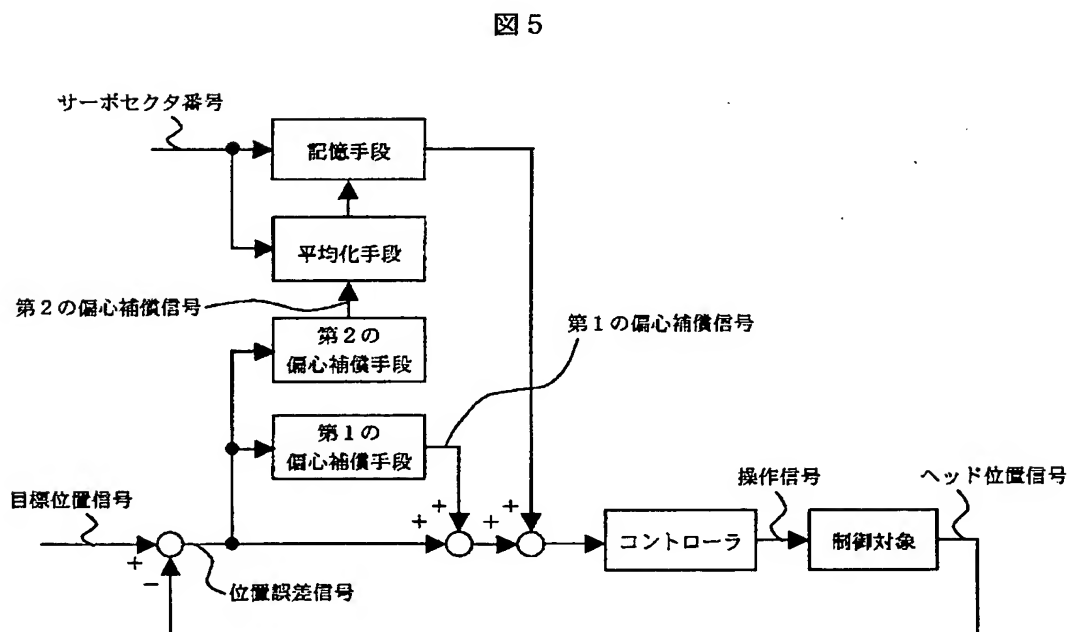
図 3

S 1	ヘッド番号	1
	セクタ番号	1
R 2	1 次ヘッド	2
	1 次セクタ	3
	2 次ヘッド	3
	2 次セクタ	4
S 3	ヘッド番号	2
	セクタ番号	5

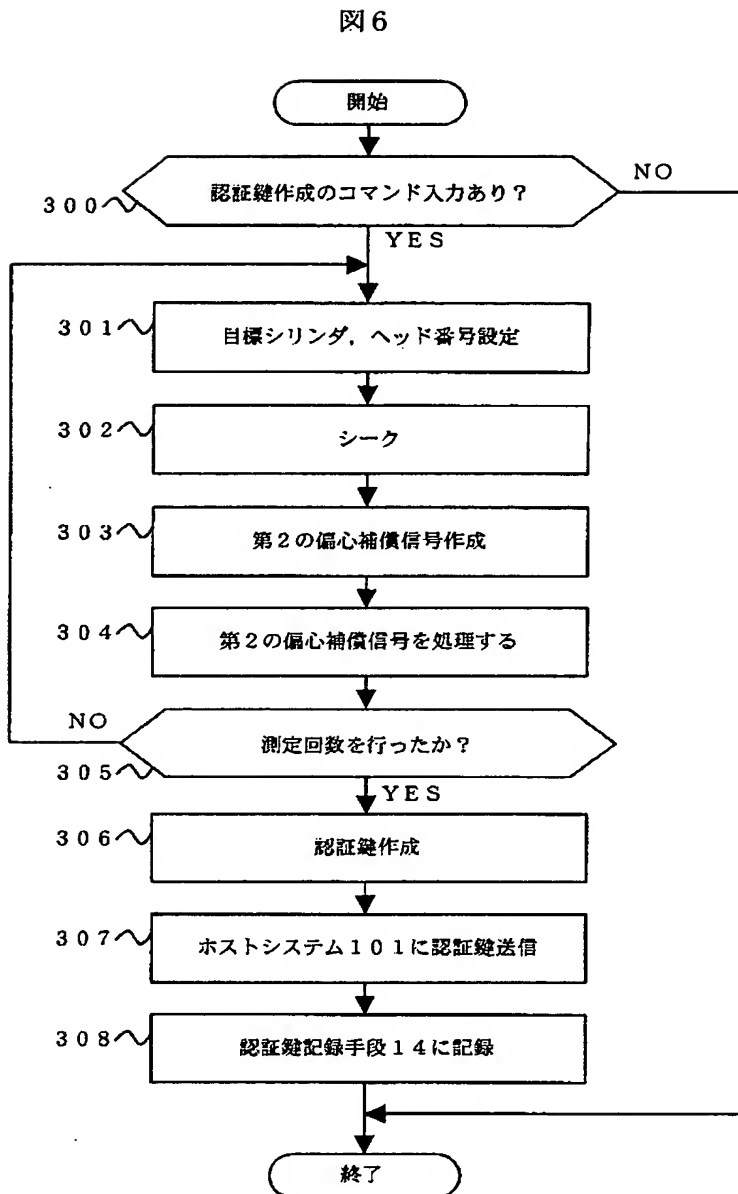
【図 4】



【図 5】

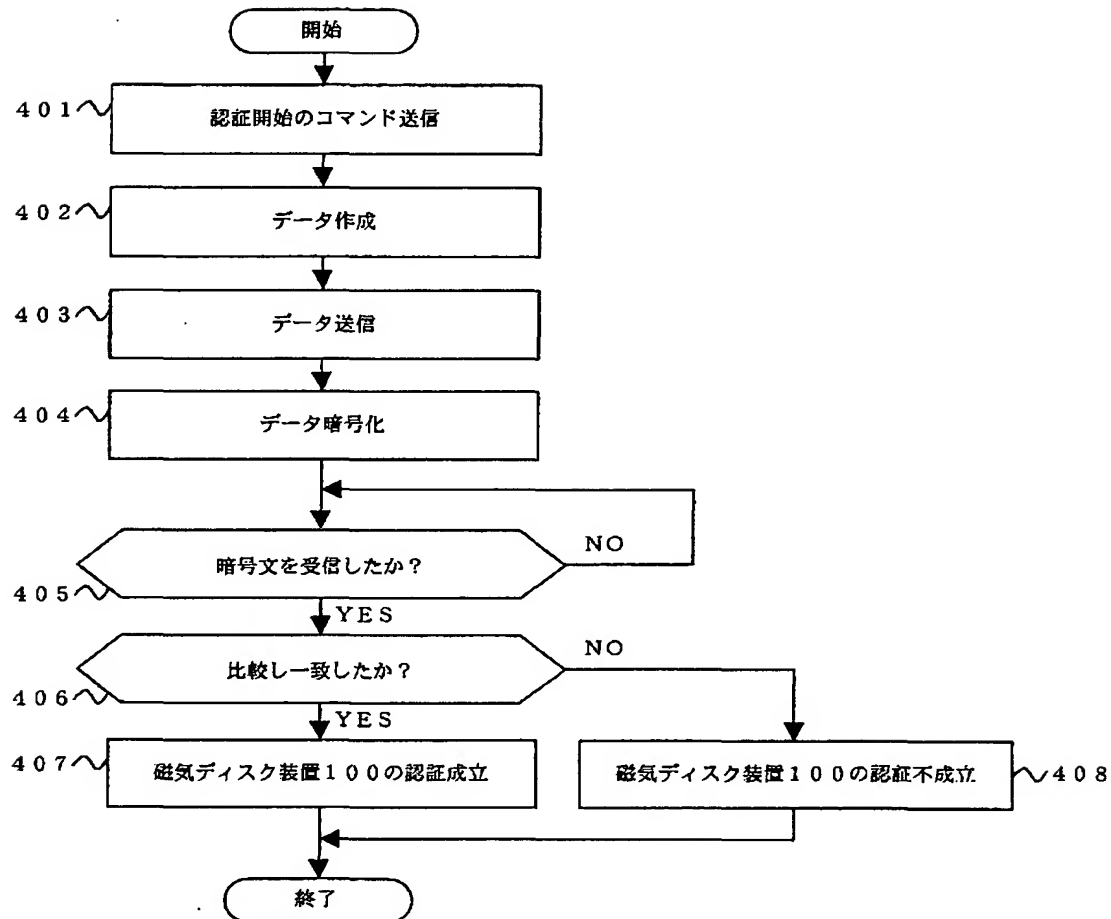


【図 6】

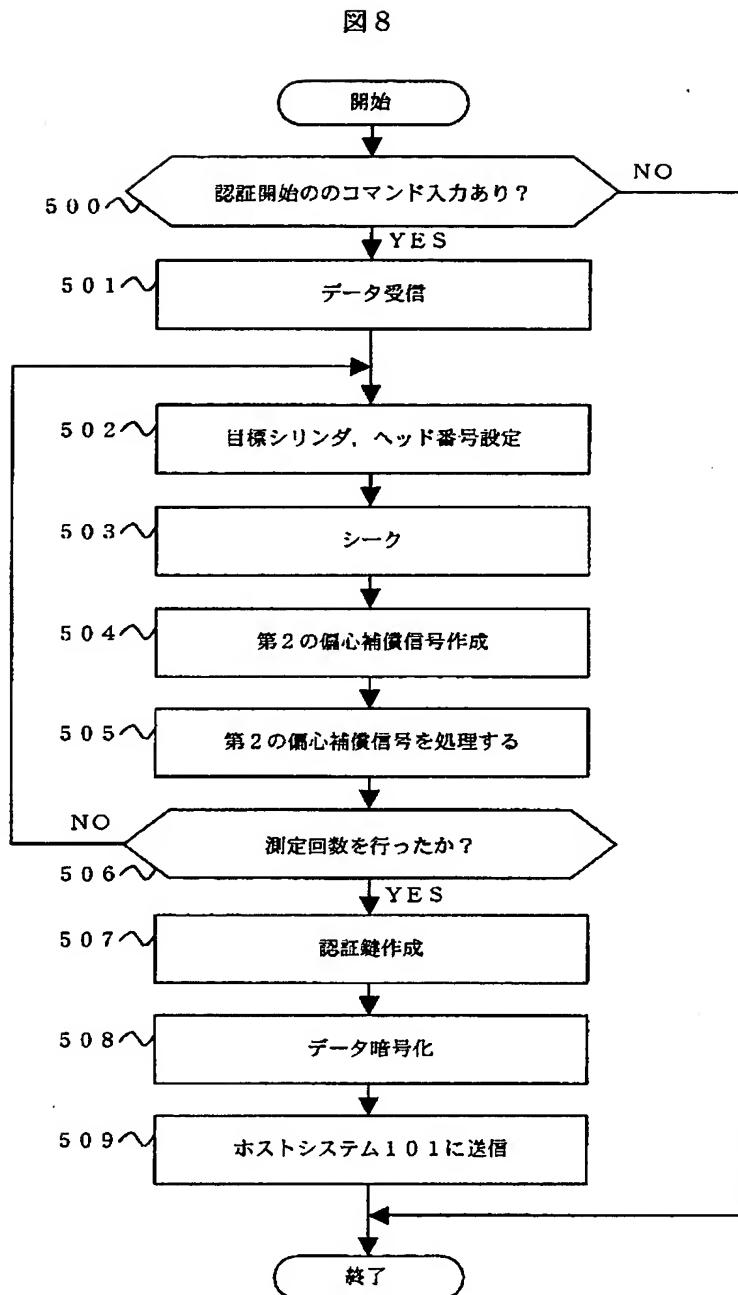


【図 7】

図 7

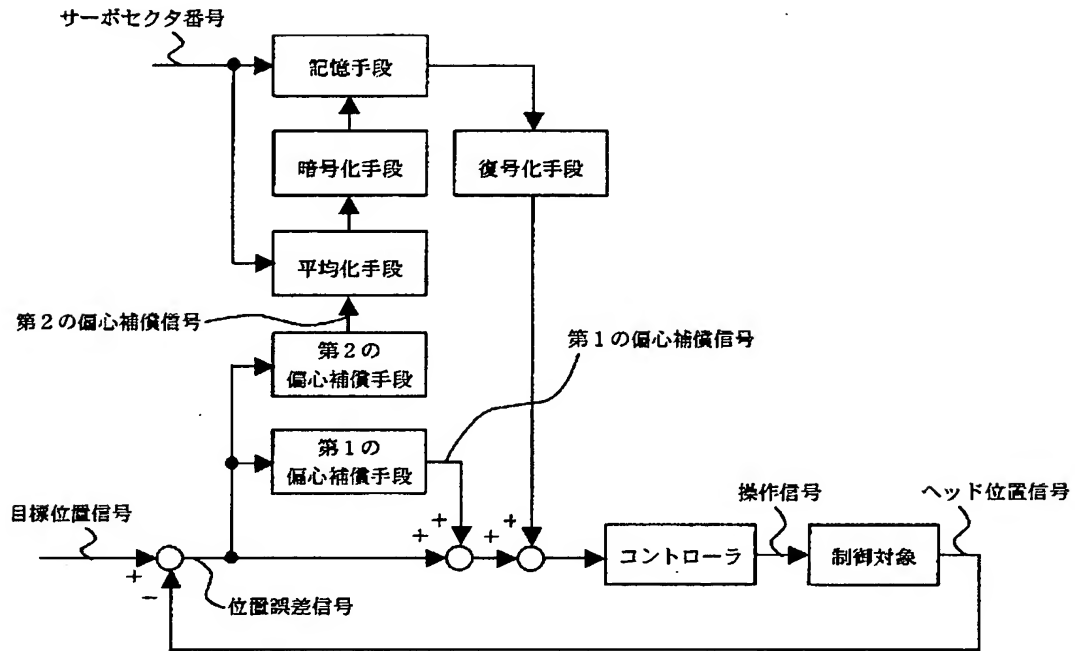


【図 8】

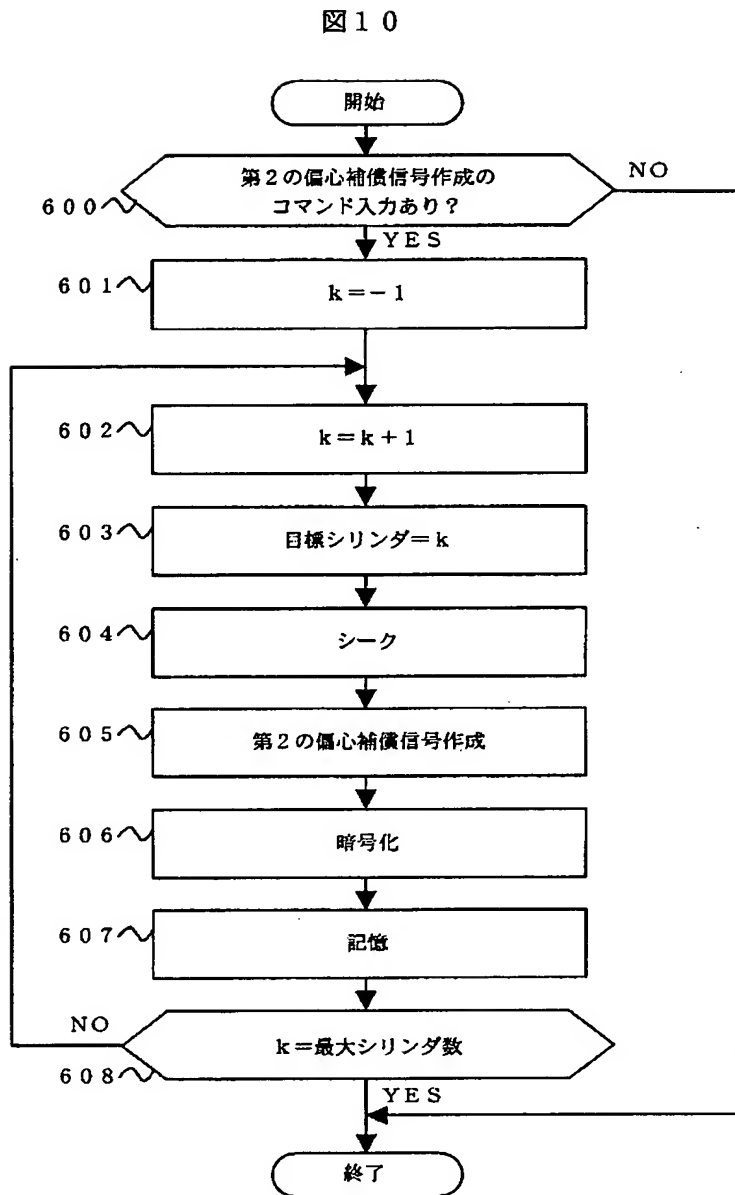


【図 9】

図 9



【図10】



【書類名】 要約書

【要約】

【課題】

磁気ディスク装置にアクセスするホストシステムを特定のものに限定可能とする情報記録再生システムを提供する。

【解決手段】

磁気ディスク装置 1 0 0 は、自身の物理的な特性に基づき認証鍵を作成する認証鍵作成手段 1 3 を有し、磁気ディスク装置 1 0 0 及びホストシステム 1 0 1 は、認証鍵を記録する認証鍵記録手段 1 4 と認証鍵に基づき認証データを作成する認証データ作成手段 1 5 とをそれぞれ有し、ホストシステム 1 0 1 の認証データと、磁気ディスク装置 1 0 0 の認証データとに基づいて、ホストシステム 1 0 1 からの磁気ディスク装置 1 0 0 の情報へのアクセスを制御する。

【選択図】 図 1

認 定 ・ 付 加 情 報

特許出願の番号	特願 2 0 0 2 - 1 8 2 3 2 5	
受付番号	5 0 2 0 0 9 1 2 3 6 6	
書類名	特許願	
担当官	第七担当上席	0 0 9 6
作成日	平成 1 4 年	6 月 2 5 日

< 認定情報・付加情報 >

【提出日】	平成14年 6月24日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日	1 9 9 0 年 8 月 3 1 日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台 4 丁目 6 番地
氏 名	株式会社日立製作所